Final draft ETSI EN 319 422 V1.1.0 (2015-12)

Electronic Signatures and Infrastructures (ESI);
Time-stamping protocol and time-stamp token profiles

Reference
DEN/ESI-0019422

Keywords
electronic signature, security, time-stamping,
trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This final draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the Vote phase of the ETSI standards EN Approval Procedure.

The present document was previously published as ETSI TS 101 861 [i.1].

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	12 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.2].

Time-stamping is critical for digital signatures in order to know whether the digital signature was affixed during the validity period of the certificate. One method of assuring the signing time is to affix a time-stamp bound to the signature as defined in IETF RFC 3161 [1].

IETF RFC 3161 [1] defines a time-stamp protocol and a time-stamp token format. The present document limits the number of options by placing some additional constraints.

1 Scope

The present document defines a profile for the time-stamping protocol and the time-stamp token defined in IETF RFC 3161 [1] including optional ESSCertIDv2 update in IETF RFC 5816 [4].

It defines what a time-stamping client supports and what a time-stamping server supports.

Time-stamp validation is out of scope and is defined in ETSI EN 319 102 [i.4].

Annex C defines media type and file-extension for time-stamp tokens.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[2] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[3] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[4] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[5] IETF RFC 7230 to RFC 7235: "Hypertext Transfer Protocol -- (HTTP/1.1)".

[6] IETF RFC 2818: "HTTP Over TLS".

[7] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 101 861: "Electronic Signatures and Infrastructures (ESI); Time stamping profile".

[i.2] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.3] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[i.4] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.5] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.6] IETF RFC 6838: "Media Type Specifications and Registration Procedures".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

time-stamp token: data object defined in IETF RFC 3161 [1], representing a time-stamp

Time-Stamping Authority (TSA): Trust Service Provider which issues time-stamp using one or more time-stamping units

Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASN	Abstract Syntax Notation
EU	Europe
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS
RFC	Request For Comments
TLS	Transport Layer Security
TSA	Time-Stamping Authority
TSU	Time-Stamping Unit

4 Requirements for a time-stamping client

4.1 Profile for the format of the request

4.1.1 Core requirement

A time-stamping client shall support the time-stamping request as defined in IETF RFC 3161 [1], clause 2.4.1 with the amendments defined in the following clauses.

4.1.2 Fields to be supported

The use of the following fields in the time-stamping request should be supported:

- the `reqPolicy`;
- the `nonce`; and
- the `certReq`.

4.1.3 Hash algorithms to be used

Hash algorithms used to hash the information to be time-stamped should be as specified in clause A.8 of ETSI TS 119 312 [i.5]. This should take into account the expected duration of the time-stamp and selected hash functions versus time given in clause 9.2 of ETSI TS 119 312 [i.5].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations.

4.2 Profile for the format of the response

4.2.1 Core requirement

A time-stamping client shall support the time-stamping response as defined in IETF RFC 3161 [1], clause 2.4.2 with the amendments defined in the following clauses.

4.2.2 Fields to be supported

The following requirements apply:

- the `accuracy` field shall be supported; and
- the `nonce` field should be supported.

A TSU needs not support ordering hence clients should not depend on the ordering of time-stamps.

If the nonce field is present in the request, the nonce field shall be present in the response with the same value.

4.2.3 Algorithms to be supported

Time-stamp token signature algorithms to be supported should be as specified in clause A.8 of ETSI TS 119 312 [i.5].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations.

4.2.4 Key lengths to be supported

Signature algorithm key lengths for the selected signature algorithm should be supported as recommended in clause 9.3 of ETSI TS 119 312 [i.5].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations.

5 Requirements for a time-stamping server

5.1 Profile for the format of the request

5.1.1 Core requirement

A time-stamping server shall support the time-stamping request as defined in IETF RFC 3161 [1], clause 2.4.1 with the amendments defined in the following clauses.

5.1.2 Fields to be supported

The following requirements apply:

- `reqPolicy` field shall be supported;
- the `nonce` field shall be supported; and
- `certReq` field shall be supported.

5.1.3 Algorithms to be supported

Hash algorithms for the time-stamp data to be supported should be as specified in clause A.8 of ETSI TS 119 312 [i.5]. This should take into account the expected duration of the time-stamp and selected hash functions versus time given in clause 9.2 of ETSI TS 119 312 [i.5].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations.

5.2 Profile for the format of the response

5.2.1 Core requirement

A time-stamping server shall support the time-stamping response as defined in IETF RFC 3161 [1], clause 2.4.2 with the amendments defined in the following clauses.

5.2.2 Fields to be supported

The requirements from IETF RFC 3161 [1], clause 2.4.2 shall apply and the following requirements apply:

- the `policy` field shall be present as an identifier for the time-stamp policy and shall conform to annex A;
- a `genTime` field shall have a value representing time with a precision necessary to support the declared accuracy shall be supported;
- the `accuracy` field shall be present and a minimum accuracy of one second shall be supported;
- the `ordering` field shall not be present or shall be set to false; and
- no extension shall be marked as critical.

The following requirement applies to the content of the `SignedData` structure in which the `TSTInfo` structure is encapsulated:

- the certificate identifier of the TSU certificate (`ESSCertID` as in IETF RFC 3161 [1] or `ESSCertIDv2` as in IETF RFC 5816 [4]) shall be included as a `signerInfo` attribute inside a `SigningCertificate` or a `SigningCertificateV2` attribute as specified in IETF RFC 5816 [4], clause 2.2.1.

5.2.3 Algorithms to be used

Hash algorithms used to hash the information to be time-stamped and time-stamp token signature algorithms should be as specified in clause A.8 of ETSI TS 119 312 [i.5].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations.

6 TSU certificate profile

6.1 General requirements

The TSU certificate shall meet the requirements defined in ETSI EN 319 412-2 [2] for the TSA being a natural person or defined in ETSI EN 319 412-3 [3] for the TSA being a legal person with the amendments defined in the following clauses.

6.2 Subject name requirements

The `countryName` attribute shall specify the country in which the TSA is established (which is not necessarily the name of the country where the TSU is located).

For a TSA being a legal person or a natural person associated with a legal person the `organizationName` shall contain the full registered name of the TSA responsible for managing the TSU. That name should be an officially registered name of the TSA.

The `commonName` specifies an identifier for the TSU. Within the TSA, the attribute `commonName` uniquely identifies the TSU used.

For a TSA being a natural person, one instance of the attribute `serialNumber` should be included in the subject field.

6.3 Key lengths requirements

The key length for the selected signature algorithm of the TSU certificate should be as recommended in clause 9.3 of ETSI TS 119 312 [i.5].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations.

6.4 Key usage requirements

The TSU certificate extended key usage setting shall be as defined in IETF RFC 3161 [1], clause 2.3.

The TSU certificate private key usage period extension should be used in order to limit the validity of the TSU's signing key.

6.5 Algorithm requirements

The TSU public key and the TSU certificate signature should use the algorithms as specified in clause A.9 of ETSI TS 119 312 [i.5].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations.

7 Profiles for the transport protocols to be supported

The time-stamping client and the time-stamping server shall support the time-stamping protocol via HTTP (IETF RFC 7230 to RFC 7235 [5]) or HTTPS (IETF RFC 2818 [6]) as defined in clause 3.4 of IETF RFC 3161 [1].

HTTPS (IETF RFC 2818 [6]) should be used instead of HTTP (IETF RFC 7230 to RFC 7235 [5]).

8 Object identifiers of the cryptographic algorithms

Object identifiers for the recommended hashing and signature algorithms are specified in ETSI TS 119 312 [i.5], clause 11.

9 Additional requirements for qualified electronic time-stamps as per Regulation (EU) No 910/2014

9.1 Regulation compliance statement

If a time-stamp token is claimed to be a qualified electronic time-stamp as per Regulation (EU) No 910/2014 [i.2], it should contain one instance of the `qcStatements` extension in the time-stamp token `extension` field with the syntax as defined in IETF RFC 3739 [i.3], clause 3.2.6.

If the `qcStatements` extension is present, it shall contain one instance of the statement "`esi4-qtstStatement-1`" as defined in annex B.

The extension `qcStatements` shall not be marked as critical.

Annex A (normative): Structure for the policy field

When the time-stamp token is issued by a TSA that conforms to ETSI EN 319 421 [7], then the `policy` field in the `TSTInfo` shall include:

- the identifier specified in clause 5.2 of ETSI EN 319 421 [7], or
- TSA's own identifier when the TSA incorporates or further constrains the policy above.

Annex B (normative): ASN.1 declarations

```
-- object identifiers
id-etsi-tsts                    OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0)
id-tst-profile(19422) 1 }
id-etsi-tsts-EuQCompliance  OBJECT IDENTIFIER ::= { id-etsi-tsts 1 }

-- statements
  esi4-qtstStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-tsts-EuQCompliance }
  --  By inclusion of this statement the issuer claims that this
  --  time-stamp token is issued as a qualified electronic time-stamp according to
  --  the REGULATION (EU) No 910/2014.
```

Annex C (normative): Time-stamp token media type and file-extension

The following media-type and file-extension are defined in accordance with IETF RFC 6838 [i.6] to identify a time-stamp token:

Media Type name:	Application
Media Subtype name:	vnd.etsi.timestamp-token
Required parameters:	none
encoding considerations:	binary
File extension:	tst

History

Document history				
V1.1.1	September 2001	Publication as ETSI TS 101 861		
V1.2.1	March 2002	Publication as ETSI TS 101 861		
V1.3.1	January 2006	Publication as ETSI TS 101 861		
V1.4.1	July 2011	Publication as ETSI TS 101 861		
V1.0.0	June 2015	EN Approval Procedure	AP 20151016:	2015-06-18 to 2015-10-16
V1.0.1	July 2015	Publication as ETSI TS 119 422		
V1.1.0	December 2015	Vote	V 20160221:	2015-12-23 to 2016-02-22